Department of Homeland Security IAIP Directorate Daily Open Source Infrastructure Report for 17 June 2005

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

For info click here
http://www.dhs.gov/

Daily Highlights

- The Department of Homeland Security has issued a Chemical Security Fact Sheet, and says that the U.S. government must impose tighter regulation of chemical facilities in order to help prevent terrorist attacks. (See item 2)

- InformationWeek reports that despite the growing problem of identity theft, most financial institutions that provide credit cards are doing an inadequate job of attacking the problem, focusing on resolution rather than prevention and detection. (See item 6)

- The Rutland Herald reports the Federal Emergency Management Agency identified five crucial deficiencies in last month's test of emergency response at Vermont Yankee nuclear power plant in Vernon, VT. (See item 22)

DHS/IAIP Update *Fast Jump*

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *June 15, University of Arkansas* — **University of Arkansas researchers to develop electrical systems for nation's power grid.** The federal government has asked engineering researchers at the University of Arkansas (UA) to develop purely electronic systems to make the nation's power grid more reliable and efficient. Silicon−carbide, solid−state equipment will replace outdated and obsolete electro−mechanical devices such as those that failed to localize the 2003

blackout in the Northeast United States, the largest and most catastrophic power failure in the history of the country. "We have to limit potentially catastrophic events so that people don't get hurt and equipment doesn't get destroyed," said Alan Mantooth, UA professor of electrical engineering and director of the newly formed National Center for Reliable Electric Power Transmission. Mantooth and three other UA electrical engineering researchers −− Juan Balda, Fred Barlow and Aicha Elshabini −− received $1 million from the U.S. Department of Energy's GridWorks Initiative to create and operate the new national center. The center's researchers, including faculty and graduate students, will design, test and package the electronic systems for future commercial use in the nation's power grid.
GridWorks Initiative: http://www.electricity.doe.gov/program/electric_rd_gridworks.cfm?section=program&level2=gridworks
Source: http://dailyheadlines.uark.edu/4915.htm

[Return to top]

Chemical Industry and Hazardous Materials Sector

2. *June 15, Bloomberg* — **DHS seeks chemical plant rules to prevent terrorism.** The U.S. government must impose tighter regulation of chemical facilities to help prevent terrorist attacks, a top official of the Department of Homeland Security (DHS) said Wednesday, June 15. “While most companies have been eager to cooperate with the department, it has become clear that the entirely voluntary efforts of these companies alone will not sufficiently address security,” said Robert Stephan, DHS assistant secretary for infrastructure protection. The American Chemistry Council, which represents 132 companies says its members already have adopted “extraordinary measures” to secure some 2,040 facilities at a cost exceeding $2 billion. Still, such companies represent only part of the chemical industry. Stephan said “high−risk” facilities representing 20 percent of U.S. chemical operating capacity aren't governed “by any kind of voluntary practice or voluntary security code.” DHS Secretary Michael Chertoff, who ordered a broad review of department policies, has concluded that “the existing patchwork of authorities does not permit us to regulate the industry effectively,” Stephan said. He said new regulations should acknowledge that many chemical plants pose little risk and that “many responsible companies” have already invested in improved security since September 11, 2001.
DHS Fact Sheet: http://www.dhs.gov/dhspublic/display?content=4543
Source: http://www.bloomberg.com/apps/news?pid=10000103&sid=axHWPE2s_Ntw&refer=us

[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

3.

June 16, Computerworld — **CheckFree knocked offline by power outage.** Customers trying to use online bill payment services through CheckFree.com on Wednesday, June 15, were deterred by a power outage that knocked the service offline for much of the day. Judy DeRango Wicks, a spokesperson for Norcross, GA−based CheckFree Corp., confirmed the service was unavailable starting at 4 a.m. and all service was restored by about 6 p.m. "We had sort of a power interruption" of an unknown cause affecting the company's facilities, Wicks said. A system of backup power generators came on automatically after the outage. "But then as we were resuming normal power production [later], without the backup, we continued to have problems," Wicks said. Technicians then turned off the power so they could identify and repair the problems, she said. Checkfree.com is an online bill payment service for about 1,600 banks, credit unions, portals, retailers and brokerage firms. It allows customers to make guaranteed payments online.
Source: http://www.computerworld.com/securitytopics/security/recovery/story/0,10801,102532,00.html

4. *June 16, Associated Press* — **Privacy advocates urge lawmakers to look overseas at lower identity theft rates.** As U.S. lawmakers mull how to cure the blight of identity theft, privacy advocates suggest they look overseas, where tighter controls on personal data and credit cards make such fraud far less common. Few experts believe other nations' data privacy laws are directly applicable to the United States, partly because the U.S. economy runs on the convenience and efficiency of a detailed credit−reporting system. However, other countries' approaches could be instructive. "We're behind much of the developed world," said Senator Charles Schumer (D−NY), who is pushing a broad bill aimed at impeding the crime. "The major European countries are doing more than we are doing, and somebody can feel safer about giving information about themselves there than in America," said Schumer. One such difference is that many countries don't use anything like Social Security numbers as universal identifiers, which serve as pass keys for criminals opening fraudulent accounts. Also, credit cards generally are harder to obtain and used less often. Perhaps most importantly, many countries don't allow financial records and other data obtained on people for one purpose to be sold or shared without their consent.
   Source: http://www.informationweek.com/showArticle.jhtml;jsessionid=BFCBD0OR2YWQQQSNDBGCKH0CJUMEKJVN?articleID=164900169

5. *June 16, Washington Post* — **FDIC alerts employees of data breach.** Thousands of current and former employees at the Federal Deposit Insurance Corp. (FDIC) are being warned that their sensitive personal information was breached, leading to an unspecified number of fraud cases. In letters dated Friday, June 10, the agency told roughly 6,000 people to be "vigilant over the next 12 to 24 months" in monitoring their financial accounts and credit reports. The data that may have been improperly accessed included names, birth dates, Social Security numbers and salary information on anyone employed at the agency as of July 2002. The agency said that in a "small number of cases," the data was used to obtain fraudulent loans from a credit union, but declined to specify how many or the credit union involved. According to the letter, the breach occurred early last year, and it remains unclear why employees were not notified for nearly 18 months. The agency wrote that it learned of the breach only "recently," but did not explain how the breach surfaced or why it took so long to learn about it. Nor did the letter say how the breach occurred, aside from stating that it was not the result of a computer security failure.

Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/06/15/AR2005061502414.html

6. *June 16, InformationWeek* — **Banks not doing enough to stop identity theft according to report.** Despite all the headlines about the growing problem of identity theft, most financial institutions that provide credit cards are doing an inadequate job of attacking the problem, focusing on resolution rather than prevention and detection, according to a report by Javelin Strategy & Research. The report ranked leading card−issuing banks based on three criteria: prevention, detection, and resolution. Issuers could score a maximum of 100 points: 40 points each for prevention and detection, and 20 points for resolution. The rankings were based on a survey of 39 banks in which researchers posing as customers asked about the bank's identity theft policies. Prevention and detection were weighted more heavily than resolution because of their greater potential benefits and cost savings. The average score for all banks was 41 points. For prevention and detection, banks achieved average scores of 16.7 and 9.7, respectively, out of a possible 40 points in each category. For resolution, banks achieved an average score of 14.4 out of a possible 20 points.
Identity Fraud Safety Scorecard for Credit Card Issuers:
http://www.javelinstrategy.com/reports/documents/JavelinIssuerSafetyScorecardBrochure05.pdf
Source: http://www.informationweek.com/showArticle.jhtml;jsessionid=BFCBD0OR2YWQQQSNDBGCKH0CJUMEKJVN?articleID=164303598

[Return to top]

Transportation and Border Security Sector

7. *June 16, USA TODAY* — **Cingular: Keep ban of cell phone calls on flights.** Cingular, the U.S.'s biggest wireless carrier, thinks cell phone conversations should continue to be banned on commercial flights while planes are airborne. The Federal Aviation Administration (FAA) is studying the possibility of relaxing the ban on the use of cellular and other wireless devices aboard commercial aircraft. Cingular last week told the agency, in so many words, that it thinks in−flight cell phone conversations are a bad idea. Cingular spokesperson Rochelle Cohen says the company is just trying to be responsive to its customers. Cohen says discourteous behavior −− talking loudly or incessantly on cell phones in the confines of a train, restaurant or other closed venues −− is a constant source of grousing by customers. Verizon Wireless, the No. 2 cell phone carrier, recently teamed with Cingular to submit comments to the Federal Communications Commission (FCC), which is examining the same issue. The FCC has long been concerned about the impact of airborne cell phone users on land−based customers. Interference is the agency's biggest concern. In their joint comments, Cingular and Verizon indicated they might be willing to support lifting the ban if safeguards existed to protect consumers on the ground from interference.
Source: http://www.usatoday.com/travel/news/2005−06−15−cell−ban−usat_x.htm

8. *June 16, Washington Business Journal* — **Independence Air marks one year.** Amid rising losses, the once profitable Atlantic Coast Airlines marked its one−year anniversary as Independence Air on Thursday, June 16. On June 16, 2004, the Washington, DC−Dulles−based carrier re−launched itself as FLYi, a discount carrier that promised to bring low−fare

competition to its Dulles hub and expand its network across the country. The airline has been successful in both, but continues to struggle financially as the industry battles competition and skyrocketing fuel costs. Independence Air has lost money every quarter since re−branding itself. Independence Air avoided a possible bankruptcy filing in February by restructuring aircraft leases when it ended 45 leases and deferred another $70 million in lease payments.
Source: http://washington.bizjournals.com/washington/stories/2005/06 /13/daily34.html

9. *June 16, Arizona Republic* — **Airfare prices rise for summer.** Packed planes and fewer frills aren't the only hazards of summer air travel this year. Airline ticket prices are up, way up in some markets. That $200 coast−to−coast fare so prevalent the past few years is largely gone except for the occasional, and limited, Internet special. The norm now for non−stop flights from Phoenix to New York, Boston and Providence, RI is $300 and higher. Southwest Airlines has not had a major fare sale since April, and America West has been quiet on the sale front, too. There are two primary reasons ultra−low fares are scarce, industry experts say: sizzling travel demand and slightly reduced competition on some routes, especially in the West. AAA and the Travel Industry Association forecast a record−breaking summer season, with a 2.3 percent increase in leisure travel. The Air Transport Association, which represents the nation's airlines, says 200 million passengers will travel on U.S. airlines this summer, up 4.1 percent from a year ago. Even though airfares are on the rise, overall fares are still about 20 percent lower in the United States than they were before the September 11, 2001 terrorist attacks.
Source: http://www.azcentral.com/arizonarepublic/news/articles/0616a irfares16.html

10. *June 15, Transportation Security Administration* — **New technology to be deployed to additional airports by September.** The Transportation Security Administration (TSA) has successfully completed the explosives detection trace portal program pilot phase for passenger screening. This new technology was tested in a pilot program in 14 cities and met TSA’s rigorous standards for excellence. TSA is eager to expand this program as an important step towards increasing explosives detection capabilities at passenger screening checkpoints at our nation’s airports. Positive feedback from participating airports, airlines and passengers indicates that the technology greatly enhances customer service. Starting in July, TSA will begin the first round of deployment by adding 44 additional machines and ten additional airports to the program. Airports in the following cities were included in the pilot program and are already using the new technology: Baltimore; Boston; Gulfport, MS; Jacksonville, FL; Las Vegas; Los Angeles; Miami; New York (JFK); Phoenix; Providence, RI; Rochester, NY; San Francisco; San Diego; and Tampa, FL. By the end of September, TSA will complete the first wave of deployment of this new technology to airports in the following cities: Charlotte, NC; Dallas (DFW); Fort Lauderdale, FL; Newark, NJ; New York (LaGuardia); Palm Beach, FL; Pittsburgh; San Juan, PR; and Washington, DC (both Dulles and Reagan National).
Source: http://www.tsa.gov/public/display?theme=44&content=090005198 0137c28

[Return to top]

Postal and Shipping Sector

11. *June 16, WTOC (GA)* — **Hazmat drill for postal workers.** An emergency drill was staged at the Postal Service Savannah, GA, Processing and Distribution Center. They evacuated the building, and taught workers about decontamination that could save their lives. U.S. Postal

Service Southeast emergency preparedness manager Jill Jacquin said, "We want them to know what they're going to experience should that alert ever go off, and being prepared and understanding the whole process makes it go a lot smoother and removes some of that fear of the alert going off." They're also adding new biohazard detection equipment at the center later this month.
Source: http://www.wtoctv.com/Global/story.asp?S=3482311&nav=0qq6b6V P

12. *June 10, Information Week* — **DHL plans identification tags for every package it ships.** DHL International GmbH this month starts developing a global IT infrastructure that will let it affix a radio−frequency identification (RFID) tag on every package it ships by 2015. DHL, the transportation and logistics arm of Deutsche Post World Net, ships more than a billion packages a year. DHL already has identified that it needs to automate IT applications, improve connectivity with customers and regulatory agencies, and work with EPCglobal Inc. members to create common standards that can be shared throughout the logistics industry. The company's IT group spends a lot of time supporting DHL's Object Name Service database, which stores information on shipped packages. Instead, DHL hopes to set up an infrastructure where RFID tags serve as links to information located elsewhere. For example, DHL believes it can reduce its data−collection and reporting requirements related to U.S. Custom declarations by using RFID tags that direct the Customs department to information within databases maintained by manufacturers that ship products. DHL plans to build an automated exception reporting layer to its infrastructure, so that RFID tags will send alerts if something unexpected occurs. For example, an RFID tag will send an alert via mobile phone or E−mail to a transportation manager if a package strays from its appointed route.
Source: http://informationweek.com/story/showArticle.jhtml?articleID =164302179

[Return to top]

Agriculture Sector

13. *June 16, News−Journal (FL)* — **Mosquito virus hits horses hard.** Mosquitoes carrying Eastern equine encephalitis led to the deaths of five horses in Volusia, FL, and two horses in Flagler, FL, over the past several months. So far, 45 horses in Florida have died this year from the disease, putting the state on pace to match 2003 when the virus killed 207 horses, state officials say. The virus tends to spread within Northeast Florida. Birds that nest near swamps pass the disease to mosquitoes, which in turn infect animals and, more rarely, humans. Heavy rainstorms have pumped up the standing water in swampy areas, prime breeding grounds for the types of mosquitoes that carry the equine disease, said Don Emminger, administrator for the East Volusia Mosquito Control District.
Source: http://www.news−journalonline.com/NewsJournalOnline/News/Flagler/03FlaglerFLAG01061605.htm

14. *June 16, Carlsbad Current−Argus (NM)* — **Disease hits New Mexico's livestock.** An outbreak of bovine trichomoniasis among beef cattle in the state has resulted in the issuance of an animal health emergency for New Mexico. The emergency health alert was issued late last month, according to the New Mexico Office of the State Veterinarian. The parasitic protozoan organism tritrichomonas fetus causes the disease in the cattle. Infection is usually detected in bulls that pass it on to cows. The infected cows are susceptible to aborting calves. Bulls, most

of which remain persistently infected, are the main reservoir for the parasite. Trichomoniasis affects all cattle but is more commonly found among beef herds. Dave Fly, New Mexico Livestock Board veterinarian, said about 10 percent of the cattle tested for the disease in the northern part of the state have tested positive. Fly noted that New Mexico is among the few Western states without strict rules regarding transporting and testing cattle across state lines and within the state. In an effort to reduce calf losses in beef cattle herds, the state is implementing a program that will make New Mexico's rules consistent with those of bordering states.
Source: http://www.currentargus.com/artman/publish/article_13611.sht ml

15. *June 15, StopSoybeanRust.com* — **New soybean rust found on kudzu in fifth Florida county.** Asian soybean rust has been found in Jefferson, FL, now the fifth rust−infected county in the state identified in 2005. The detection is on kudzu leaves and was confirmed by three different means: microscopy by the University of Florida/Institute of Food and Agricultural Sciences; enzyme−linked immunosorbant assay (ELISA) by UF/Plant Pathology; and real−time polymerase chain reaction (PCR) by the University of Florida/Plant Disease Clinic. Jefferson County is one county east of Tallahassee's home county (Leon) in north−central Florida. That's just south across the border (and two counties east) from Seminole County, Georgia, where rust has been found in two locations on volunteer soybeans.
Source: http://www.stopsoybeanrust.com/viewStory.asp?StoryID=374

[Return to top]

Food Sector

16. *June 15, Food Safety and Inspection Service* — **Chicken salad recalled.** Sally Sherman Foods, a Mount Vernon, NY, firm, is voluntarily recalling approximately 5,065 pounds of chicken salad that may be contaminated with Listeria monocytogenes, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced Wednesday, June 15. The products were distributed to restaurants, retail stores and other institutions in Connecticut, Louisiana, Maryland, Massachusetts, New Jersey, New York, Rhode Island and Vermont. The problem was discovered through routine FSIS microbial sampling. FSIS has received no reports of illnesses associated with consumption of these products. Consumption of food contaminated with Listeria monocytogenes can cause listeriosis, an uncommon but potentially fatal disease.
Source: http://www.fsis.usda.gov/News_&_Events/Recall_027_2005_Relea se/index.asp

[Return to top]

Water Sector

Nothing to report.

[Return to top]

Public Health Sector

17. *June 16, Voice of America* — **Indonesia reports first human case of bird flu.** A poultry farm worker in Indonesia has become the country's first confirmed victim of the potentially deadly

bird flu virus. The discovery makes Indonesia the fourth country in which the virus has crossed from animals to humans since the latest outbreak in 2003. The H5N1 strain of avian virus has killed at least 55 people in three different Southeast Asian countries since January of 2003, but the case discovered on the island of Sulawesi is the first to be found in Indonesia. The case was discovered after poultry on the farm where the victim worked became infected. Tests later showed that the man was carrying antibodies for the virus. Although the man has shown no symptoms and is no longer infected, the presence of antibodies means he was at one time a carrier of the disease.
Source: http://www.voanews.com/english/2005−06−16−voa9.cfm

18. *June 16, Jakarta Post (Indonesia)* — **Seven new polio cases found in Indonesia.** The World Health Organization (WHO) said on Thursday, June 16, that seven new cases of polio have been discovered in Indonesia, bringing the total number of people suffering from the disease to 46. The WHO said that seven new cases had been confirmed in West Java in the same region as an initial diagnosis in late April that prompted the campaign to vaccinate 6.4 million children. Two of the seven new cases were in Sukabumi, the area where the original outbreak was detected, WHO said in a statement. The other five were in Bogor and Lebak. WHO says that nearly 500 new polio cases have been confirmed worldwide this year, and that Yemen is the worst hit nation, with 220 cases.
Source: http://www.thejakartapost.com/detaillatestnews.asp?fileid=20 050616145135&irec=7

19. *June 16, San Jose Mercury News (CA)* — **Chiron warns it will make fewer flu shots.** Chiron, the biotechnology firm blamed for last winter's flu vaccine shortage, announced Wednesday, June 15, that delays in production at its plant in England will result in fewer doses than it had said it would make available for the coming flu season. The company estimates it will make only 18 million to 26 million doses of its Fluvirin brand vaccine instead of the 25 million to 30 million doses it promised after British health authorities allowed it to reopen its factory in Liverpool on March 2. The facility was closed in October 2004 when inspectors found contamination, creating a critical shortage of 50 million doses of flu vaccine available to the U.S. public health system.
Source: http://www.siliconvalley.com/mld/siliconvalley/11909558.htm

20. *June 16, Associated Press* — **New flu vaccine shows good results.** Drug maker MedImmune Inc. said Thursday, June 16, that preliminary results show that a late−stage clinical study met its primary endpoint in comparing a new flu vaccine to its FluMist vaccine. The main objective of the Phase III clinical trial was to see if the investigational vaccine CAIV−T produced an equivalent immune response to the company's FluMist vaccine, which was approved by the Food and Drug Administration (FDA) in June 2003. The CAIV−T vaccine is a new formulation that remains stable in a refrigerator, unlike FluMist, which must be stored in a freezer. The company said that it will further analyze the data and submit it to the FDA later in the year. "Completing this Phase 3 study is the key step in our plan to seek U.S. regulatory approval for CAIV−T in healthy individuals five to 49 years of age and replace the frozen formulation of FluMist in the marketplace," said Edward M. Connor, chief medical officer, in a statement. "Additional studies are ongoing to assess CAIV−T compared to the injectable flu vaccine in children from six months to five years of age."
Source: http://www.forbes.com/work/feeds/ap/2005/06/16/ap2097061.htm l

[Return to top]

Government Sector

Nothing to report.

[Return to top]

Emergency Services Sector

21. *June 16, Asbury Park Press (NJ)* — **New Jersey's 18 Mile Emergency Services Association hosts first drill ever.** Emergency crews in Surf City, NJ learned there are some glitches in the communications system when trying to coordinate apparatus and personnel from five fire companies and three first aid squads when they conducted their first drill ever on Tuesday, June 14. The drill, sponsored by the 18 Mile Emergency Services Association, was declared a success when 40 emergency services personnel from one end of Long Beach Island to the other responded to a mock ocean rescue consisting of an overturned boat with four victims in the water about 50 yards from shore. Communication coordination was the biggest problem. Surf City Fire Chief Brian Fullerton said that fire units, EMS operations, fire police, and command control were all on different radio channels. Furthermore, access to the beach was initially cut off by responding ambulances at the scene. Fullerton stated, "It took some time to get used to the communications equipment, but that is to be expected when there are different agencies involved". Fullerton said the 18 Mile Emergency Services Association would hold another drill in September.
Source: http://www.app.com/apps/pbcs.dll/article?AID=/20050616/NEWS02/506160522/1070/NEWS03

22. *June 16, Rutland Herald (VT)* — **FEMA issues Vermont a harsh review of nuclear drill.** The Federal Emergency Management Agency (FEMA) identified five crucial deficiencies in last month's test of emergency response at Vermont Yankee nuclear power plant in Vernon, VT. Three of the five deficiencies were cited in the state's Emergency Operations Center in Waterbury, and one each against the towns of Vernon and Halifax. Kenneth Horak, acting regional director of FEMA in Boston, stated that the emergency operations center had a 14−minute delay in sending out an evacuation notice to the residents of Vernon and Guilford, as well as a warning to the towns of Brattleboro, Dummerston, and Halifax to seek shelter. Horak also said the State sent out public information messages that were "misleading, inaccurate, lacked direction and in many instances it was contradictory, confusing and incomplete." Vernon's problem centered on a warning siren that was eight minutes late according to Horak. He added that one Vernon selectman filled in for the emergency director and "without proper training and experience, he was not prepared to direct and control the organization." In Halifax, town officials took too long to complete their emergency notification route, according to FEMA. According to FEMA, the State and towns at fault must correct the problems within 120 days.
Source: http://www.rutlandherald.com/apps/pbcs.dll/article?AID=/20050616/NEWS/506160380/1003

23. *June 16, Capital Times (WI)* — **Crews respond to 'hijacking emergency' drill at Wisconsin airport.** About 200 emergency, law enforcement and facilities personnel from 40 agencies converged at Dane County Regional Airport in Dane County, WI, for a mock hijacking drill in order to practice their disaster training in a full−scale emergency. Federal regulations require the airport to have a full−scale exercise every three years. The exercise started at 8 a.m. when air traffic control notified emergency crews at Dane County Regional Airport that Last Resort Airlines Flight 9976, which had just taken off from the airport, was returning because of engine problems. Three "terrorists" on board soon realized they weren't going to the nation's capital and then took the 70 passengers hostage. Within minutes, law enforcement and emergency personnel were on the scene. About a dozen hostages were released, but two hijackers killed themselves when negotiations broke down, while a third "sleeper" terrorist sprayed passengers with sodium cyanide before also committing suicide. By 11 a.m., the plane was cleared, injured passengers were on their way to area hospitals and the "crisis" was over. Eric Dahl, public information officer of the Madison Fire Department, said the exercise gives local agencies the chance to work together as a team.
Source: http://www.madison.com/tct/news/index.php?ntid=43801&ntpid=1

24. *June 14, Government Technology* — **National Technology Alliance awards GUARD Program.** The Geospatially−Aware Urban Approaches for Responding to Disasters (GUARD) program was recently awarded to Rosettex Technology and Ventures Group by the National Technology Alliance (NTA). NTA is a U.S. Government program established to discover, initiate, and accelerate commercial technology development to meet U.S. national security and defense technology needs. The GUARD will create dependable, two−way wireless communications networks in urban areas so that first responders can work more effectively during natural disasters or man−made emergencies. GUARD builds on two prior years of prototyping and demonstration as the "Smart Dissemination Networks" (Smart Nets) program. GUARD extends the capabilities, team, and technologies already in place to establish a pre−operational prototype in New York City, a second interconnected regional solution in St. Louis, and a third in Washington, DC, or Las Vegas. Smart Nets makes use of the Educational Broadband Service Band (EBS). This feature provides dependable two−way wireless broadband communications to fire, police, and other emergency personnel in the field by providing dramatically wider, licensed bandwidth than conventional emergency response communications systems.
Source: http://www.govtech.net/magazine/channel_story.php/94293

[Return to top]

Information Technology and Telecommunications Sector

25. *June 16, vnunet* — **United Kingdom's cyber infrastructure under Trojan attack.** Parts of the United Kingdom's (UK) key computer systems are being targeted by Trojan software apparently originating from the Far East, according to the National Infrastructure Security Coordination Centre (NISCC). Both the UK government and private companies are being targeted, and an NISCC bulletin lists 76 Trojan programs that have been detected. The organization claims that the IP addresses on the e−mails often come from the Far East. "Trojan capabilities suggest that the covert gathering and transmitting of otherwise privileged information is a principal goal," stated the bulletin. "The attacks normally focus on individuals

who have jobs working with commercially or economically sensitive data." The bulletin also warned that firewalls and antivirus software do not protect against the Trojans as they can be modified by security code to avoid signature traces.
NISCC Bulletin: http://www.niscc.gov.uk/niscc/docs/ttea.pdf
Source: http://www.vnunet.com/vnunet/news/2138105/uk−infrastructure− trojan−attack

26. *June 15, FrSIRT* — **Bitrix Site Manager remote PHP file inclusion vulnerability.** A vulnerability was identified in Bitrix Site Manager, which may be exploited by attackers to compromise a vulnerable web server. This flaw is due to an input validation error in the "index.php" script when processing a specially crafted "SERVER[DOCUMENT_ROOT]" variable, which may be exploited by attackers to include arbitrary files and execute remote commands with the privileges of the web server. There is no solution at this time.
Source: http://www.frsirt.com/english/advisories/2005/0779

27. *June 15, SecurityFocus* — **ViRobot Linux Server remote buffer overflow vulnerability.** ViRobot Linux Server is prone to a remote buffer overflow vulnerability affecting the Web based management interface. This issue presents itself because the application fails to perform boundary checks prior to copying user supplied data into sensitive process buffers. An attacker can gain unauthorized access to a vulnerable computer by supplying malformed values through cookies. There is no solution at this time.
Source: http://www.securityfocus.com/bid/13964/exploit

28. *June 15, CNET News* — **New worm hits AOL instant messaging network.** A new worm spread quickly on America Online's AIM instant messaging service Wednesday afternoon, June 15, but was contained within hours, experts said. The worm spread in instant messages with the text: "LOL LOOK AT HIM" and included a Web link to a file called "picture.pif." If that file was downloaded and opened, the worm would send itself to all contacts on the victim's AIM Buddy List, according to representatives from IM security companies Facetime and IMlogic. Both IMlogic and Facetime were investigating the picture.pif file to determine exactly what it does. Facetime and IMlogic received several inquiries on the worm, signaling that it was widespread. The worm hit employees at Hewlett−Packard and prompted tech support at the company to send out an alert to employees. The worm is the latest in an increasing number of cyberthreats that use instant messaging to attack Internet users. Just as with attachments and links in e−mail, instant message users should be careful when clicking on links that arrive in instant messages−−even messages from people they know, experts have warned.
Source: http://news.com.com/New+worm+hits+AIM+network/2100−7349_3−57 48646.html

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT reports Microsoft Security

Bulletins for June, 2005 address a number of vulnerabilities in Windows, Internet Explorer, Outlook Express, Outlook Web Access, ISA Server, the Step by Step Interactive Training engine, and telnet. Exploitation of the most serious of these vulnerabilities could allow a remote, unauthenticated attacker to execute arbitrary code with SYSTEM privileges. This would allow an attacker to take complete control of a vulnerable system. An attacker could also execute arbitrary code with user privileges, or cause a denial of service. Further information about the more serious vulnerabilities is available at URL: http://www.us−cert.gov/cas/techalerts/TA05−165A.html

Current Port Attacks

Top 10 Target Ports	445 (microsoft−ds), 135 (epmap), 6881 (bittorrent), 27015 (halflife), 1026 (−−−), 53 (domain), 139 (netbios−ssn), 25 (smtp), 1434 (ms−sql−m), 137 (netbios−ns) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.

[Return to top]

General Sector

29. *June 16, Associated Press* — **Spain arrests 11 terror suspects .** Spanish police arrested 11 men Wednesday, June 15, on charges of belonging to a Syrian−based network that recruited suicide bombers to attack U.S. troops in Iraq, officials said. Five other people were detained a day earlier in connection with last year's train bombings in Madrid that killed 191 people and wounded more than 1,500, authorities said. More than 500 heavily armed police staged pre−dawn raids in a half dozen cities to grab the 11 alleged members of a recruiting network that has ties to Abu−Musab al−Zarqawi's terror group al−Qaeda in Iraq, the Interior Ministry said. Spain has had several brushes with al−Qaeda, including commuter train bombings on March 11, 2004, a reported plot to blow up a Madrid courthouse last year, and militants' alleged use of Spain to organize the September 11, 2001, attacks on America. But this was the first time Spain arrested people on suspicion of sending suicide attackers to Iraq, officials at the National Court said. Most of the 11 are Moroccan and practically all of them sold drugs and staged robberies to finance their network, the ministry said.
Source: http://www.fortwayne.com/mld/fortwayne/news/local/11909134.h tm

[Return to top]

DHS/IAIP Products & Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures:

DHS/IAIP Daily Open Source Infrastructure Reports − The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS/IAIP Daily Open Source Infrastructure Report is available on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

Homeland Security Advisories and Information Bulletins − DHS/IAIP produces two levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that addresses cyber and/or infrastructure dimensions with possibly significant impact. Homeland Security Advisories and Information Bulletins are available on the Department of Homeland Security Website: http://www.dhs.gov/dhspublic/display?theme=70

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 983−3644 for more information.

Contact DHS/IAIP

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

DHS/IAIP Disclaimer

The DHS/IAIP Daily Open Source Infrastructure Report is a non−commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.